

02.02.01

JP 01/772 日本国特許庁

PATENT OFFICE  
JAPANESE GOVERNMENT

#4

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

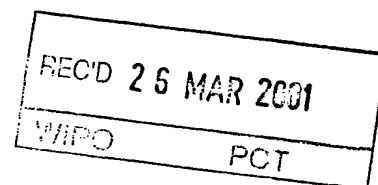
2000年 8月 7日

出願番号  
Application Number:

特願2000-238077

出願人  
Applicant(s):

ソニー株式会社



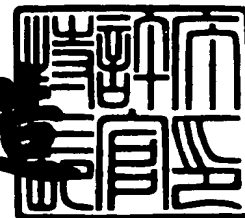
09/937797

PRIORITY  
DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2001年 3月 2日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2001-3015167

【書類名】 特許願

【整理番号】 0000460905

【提出日】 平成12年 8月 7日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/30

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
                                内

    【氏名】 橋本 主税

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
                                内

    【氏名】 佐竹 清

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
                                内

    【氏名】 金巻 裕史

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
                                内

    【氏名】 齋藤 真

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

    【識別番号】 100094053

    【弁理士】

    【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録方法、情報復元方法およびそれらの装置と記録媒体

【特許請求の範囲】

【請求項 1】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

情報記録方法。

【請求項 2】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 1 に記載の情報記録方法。

【請求項 3】

前記所定の情報を暗号化し、

当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する

請求項 1 に記載の情報記録方法。

【請求項 4】

前記複数のモジュールをそれぞれ暗号化し、

当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

請求項 1 に記載の情報記録方法。

【請求項 5】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、

当該読み出したモジュールを合成して前記所定の情報を復元する

情報復元方法。

【請求項 6】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 5 に記載の情報復元方法。

【請求項 7】

前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する  
請求項 5 に記載の情報復元方法。

【請求項 8】

前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する  
請求項 5 に記載の情報復元方法。

【請求項 9】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段と

を有する情報記録装置。

【請求項 10】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 9 に記載の情報記録装置。

【請求項 11】

前記所定の情報を暗号化する暗号化手段

をさらに有し、

前記情報分割手段は、

前記暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する

請求項 9 に記載の情報記録装置。

【請求項 12】

前記複数のモジュールをそれぞれ暗号化する暗号化手段  
をさらに有し、  
前記書き込み手段は、  
前記暗号化によって得られた複数のモジュールを相互に異なる記録媒体または  
同一の記録媒体の異なる領域に書き込む  
請求項 9 に記載の情報記録装置。

【請求項 1 3】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に  
異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合  
に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モ  
ジュールを読み出す読み出し手段と、

当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段  
と

を有する情報復元装置。

【請求項 1 4】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に  
相互に独立している記録媒体である

請求項 1 3 に記載の情報復元装置。

【請求項 1 5】

前記合成して得た情報を復号する復号手段

をさらに有する

請求項 1 3 に記載の情報復元装置。

【請求項 1 6】

前記読み出したモジュールを復号する復号手段

をさらに有し、

前記情報合成手段は、前記復号したモジュールを合成して前記所定の情報を復  
元する

請求項 1 3 に記載の情報復元装置。

【請求項 1 7】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録された

記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、記録媒体に保持される情報の秘匿性を高めることができる情報記録方法、情報復元方法およびそれらの装置に関する。

【0002】

【従来の技術】

近年、電子商取引の発達に伴い、ユーザの個人ID情報や暗証番号、取引の履歴情報、ユーザの名前、住所、経歴および職業などの個人情報などの秘匿性のある情報を、サーバ装置や端末装置などが管理するケースが多くなっている。

【0003】

サーバ装置や端末装置では、例えば、特開平11-2726781号公報に示されるように、上述したような秘匿性のある情報を、所定の暗号鍵で暗号化して、コンピュータに内蔵されたHDD(Hard Disk Drive)や、携帯性のあるCD-ROM、フロッピーディスク、PCカードなどの記録媒体に記録している。

【0004】

【発明が解決しようとする課題】

しかしながら、上述した従来のサーバ装置や端末装置では、通常、秘匿性のある情報を単体の記録媒体に記録しており、その記録媒体が盗まれたり、不正にコピーされると、当該情報の秘匿性が失われてしまうという問題がある。

このような秘匿性のある情報は、通常、暗号化されて記録媒体に記録されるが、暗号化は復号（解読）される可能性があり、秘匿性を保持する上で十分ではない。

【0005】

本発明は上述した従来技術の問題点に鑑みてなされ、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法、情報復元方法およびそれらの装置と記録媒体に関する。

【 0 0 0 6 】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第 1 の発明の情報記録方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

【 0 0 0 7 】

また、第 1 の発明の情報記録方法は、好ましくは、前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

【 0 0 0 8 】

また、第 1 の発明の情報記録方法は、好ましくは、前記所定の情報を暗号化し、当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する。

【 0 0 0 9 】

また、第 1 の発明の情報記録方法は、好ましくは、前記複数のモジュールをそれぞれ暗号化し、当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

【 0 0 1 0 】

また、第 2 の発明の情報復元方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、当該読み出したモジュールを合成して前記所定の情報を復元する。

【 0 0 1 1 】

また、第 2 の発明の情報復元方法は、好ましくは、前記複数のモジュールが記



録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

【0012】

また、第2の発明の情報復元方法は、好ましくは、前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する。

【0013】

また、第2の発明の情報復元方法は、好ましくは、前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する。

【0014】

また、第3の発明の情報記録装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段とを有する。

【0015】

また、第4の発明の情報復元装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段とを有する。

【0016】

また、第5の発明の記録媒体は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録されている。

【0017】

【発明の実施の形態】

以下、本発明の実施形態に係わる情報記録装置および情報復元装置について説明する。

第1実施形態

図1は、本実施形態の情報記録装置1の構成図である。

図1に示すように、情報記録装置1は、読み出し回路10、暗号化回路11、情報分割回路12、書き込み回路13、14を有する。

情報記録装置1は、記録媒体15から読み出した個人情報D1を暗号化した後に、それぞれを単独では個人情報D1の秘匿性が保持される2つのモジュールD3、D4に分割し、モジュールD3を記録媒体16に書き込み、モジュールD4を記録媒体17に書き込む。

本実施形態において、記録媒体15、16、17は、HDD装置や、携帯性のあるCD-ROM、フロッピーディスク、PCカードなどの記録媒体である。

#### 【0018】

読み出し回路10は、記録媒体15から読み出した個人情報D1を暗号化回路11に出力する。

個人情報D1は、図2に示すように、情報Data1～DataNからなる。

また、個人情報D1は、例えば、ユーザの個人ID情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

#### 【0019】

暗号化回路11は、所定の暗号鍵を用いて、読み出し回路10から入力した個人情報D1を暗号化して個人情報D2を生成し、これを情報分割回路12に出力する。

暗号化された個人情報D2は、図2に示すように、それぞれ情報Data1～DataNを暗号化した情報Data1'～DataN'からなる。

#### 【0020】

情報分割回路12は、暗号化回路11から入力した暗号化された個人情報D2を、それぞれを単独では個人情報D1の秘匿性が保持される2つのモジュールD3、D4に分割し、モジュールD3を書き込み回路13に出力し、モジュールD4を書き込み回路14に出力する。

図2に示すように、情報分割回路12は、情報D2内の情報Data1'～DataN'を、それぞれ情報Data1A'およびData1B'、情報Data

a 2 A' および Data 2 B'、情報 Data 3 A' および Data 3 B'、  
...、情報 Data K A' および Data K B'、...、情報 Data N  
A' および Data N B' に分割する。

そして、情報分割回路 12 は、情報 Data 1 A'、Data 2 A'、Data  
3 A'、...、Data K A'、...、Data N A' からなるモジュール  
D 3 を書き込み回路 13 に出力する。

また、情報分割回路 12 は、情報 Data 1 B'、Data 2 B'、Data  
3 B'、...、Data K B'、...、Data N B' からなるモジュール  
D 4 を書き込み回路 14 に出力する。

【0021】

書き込み回路 13 は、情報分割回路 12 から入力したモジュール D 3 を記録媒  
体 16 に書き込む。

【0022】

書き込み回路 14 は、情報分割回路 12 から入力したモジュール D 4 を記録媒  
体 17 に書き込む。

【0023】

以下、情報記録装置 1 の動作を説明する。

図 3 は、情報記録装置 1 の動作を説明するためのフローチャートである。

【0024】

ステップ ST 11:

読み出し回路 10 によって、記録媒体 15 から図 2 に示す個人情報 D 1 が読み  
出されて暗号化回路 11 に出力される。

【0025】

ステップ ST 12:

暗号化回路 11 において、所定の暗号鍵を用いて、読み出し回路 10 から入力  
された個人情報 D 1 が暗号化されて図 2 に示す個人情報 D 2 が生成され、当該個  
人情報 D 2 が情報分割回路 12 に出力される。

【0026】

ステップ ST 13:

情報分割回路 12 において、暗号化回路 11 から入力された個人情報 D2 が、それぞれを単独では個人情報 D1 の秘匿性が保持される図 2 に示す 2 つのモジュール D3, D4 に分割される。

そして、情報分割回路 12 から書き込み回路 13 にモジュール D3 が出力され、情報分割回路 12 から書き込み回路 14 にモジュール D4 が出力される。

【0027】

ステップ ST14 :

書き込み回路 13 によって、モジュール D3 が記録媒体 16 に書き込まれる。

書き込み回路 14 によって、モジュール D4 が記録媒体 17 に書き込まれる。

【0028】

以上説明したように、情報記録装置 1 によれば、図 2 に示すように、個人情報 D1 が、暗号化された後に、それぞれを単独では個人情報 D1 の秘匿性が保持される 2 つのモジュール D3, D4 に分割され、モジュール D3, D4 がそれぞれ物理的に独立した記録媒体 16, 17 にそれぞれ記録される。

そのため、記録媒体 16, 17 を別々に保管すれば、記録媒体 16, 17 の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報 D1 の秘匿性は保たれる。

【0029】

## 第 2 実施形態

図 4 は、本実施形態の情報復元装置 31 の構成図である。

情報復元装置 31 は、上述した第 1 実施形態の情報記録装置 1 によって、記録媒体 16 と 17 とに分割して記録された個人情報から、本来の個人情報 D1 を復元する。

図 4 に示すように、情報復元装置 31 は、読み出し回路 20、, 21、情報合成回路 22、復号回路 23 および書き込み回路 24 を有する。

図 4 において、記録媒体 16 および 17 には、前述した第 1 実施形態で説明した図 3 に示す処理を経て、それぞれモジュール D3 および D4 が記録されている。

【0030】

読み出し回路 20 は、記録媒体 16 から読み出したモジュール D3 を情報合成回路 22 に出力する。

【0031】

読み出し回路 21 は、記録媒体 17 から読み出したモジュール D4 を情報合成回路 22 に出力する。

【0032】

情報合成回路 22 は、図 5 に示すように、読み出し回路 20 から入力したモジュール D3 と、読み出し回路 21 から入力したモジュール D4 とを合成して個人情報 D2 を生成し、これを復号回路 23 に出力する。

【0033】

復号回路 23 は、情報合成回路 22 から入力した個人情報 D2 を、所定の復号鍵を用いて復号して個人情報 D1 を生成し、これを書き込み回路 24 に出力する。

【0034】

書き込み回路 24 は、復号回路 23 から入力した個人情報 D1 を、記録媒体 15 に書き込む。

【0035】

以下、情報復元装置 31 の動作を説明する。

図 6 は、情報復元装置 31 の動作を説明するためのフローチャートである。

【0036】

ステップ ST21 :

読み出し回路 20 によって、記録媒体 16 から図 5 に示すモジュール D3 が読み出されて情報合成回路 22 に出力される。

また、読み出し回路 21 によって、記録媒体 17 から図 5 に示すモジュール D4 が読み出されて情報合成回路 22 に出力される。

【0037】

ステップ ST22 :

情報合成回路 22 において、図 5 に示すように、読み出し回路 20 から入力したモジュール D3 と、読み出し回路 21 から入力したモジュール D4 とが合成さ

れて個人情報D 2 が生成される。

個人情報D 2 は、情報合成回路 2 2 から復号回路 2 3 に出力される。

【 0 0 3 8 】

ステップ S T 2 3 :

復号回路 2 3 において、情報合成回路 2 2 から入力した個人情報D 2 が、所定の復号鍵を用いて復号して個人情報D 1 を生成され、これが書き込み回路 2 4 に出力される。

【 0 0 3 9 】

ステップ S T 3 4 :

書き込み回路 2 4 によって、復号回路 2 3 から入力した個人情報D 1 が記録媒体 1 5 に書き込まれる。

【 0 0 4 0 】

以上説明したように、情報復元装置 3 1 によれば、正当な者が当該装置を用いることで、前述した第 1 実施形態の情報記録装置 1 によって別々の記録媒体 1 6 , 1 7 に格納されたモジュールD 3 , D 4 から個人情報D 1 を復元できる。

【 0 0 4 1 】

### 第 3 実施形態

図 7 は、本実施形態の情報記録装置 4 1 の構成図である。

図 7 に示すように、情報記録装置 4 1 は、読み出し回路 5 0、情報分割回路 5 1、暗号化回路 5 2、5 3 および書き込み回路 5 4、5 5 を有する。

情報記録装置 4 1 は、記録媒体 1 5 から読み出した個人情報D 1 を、それぞれを単独では個人情報D 1 の秘匿性が保持される 2 つのモジュールD 1 2、D 1 3 に分割した後に暗号化してモジュールD 1 4、D 1 5 を生成し、モジュールD 1 4 を記録媒体 1 6 に書き込み、モジュールD 1 5 を記録媒体 1 7 に書き込む。

【 0 0 4 2 】

読み出し回路 5 0 は、記録媒体 1 5 から読み出した個人情報D 1 を情報分割回路 5 1 に出力する。

個人情報D 1 は、図 8 に示すように、情報D a t a 1 ~ D a t a N からなる。

また、個人情報D 1 は、例えば、ユーザの個人 I D 情報や暗証番号、取り引き

の履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

【0043】

情報分割回路51は、読み出し回路50から入力した個人情報D1を、それぞれを単独では個人情報D1の秘匿性が保持される2つのモジュールD12、D13に分割し、モジュールD12を暗号化回路52に出力し、モジュールD13を暗号化回路53に出力する。

図8に示すように、情報分割回路51は、情報D1内の情報Data1～DataNを、それぞれ情報Data1AおよびData1B、情報Data2AおよびData2B、情報Data3AおよびData3B、……、情報DataKAおよびDataKB、……、情報DataNAおよびDataNBに分割する。

そして、情報分割回路51は、情報Data1A、Data2A、Data3A、……、DataKA、……、DataNAからなるモジュールD12を暗号化回路52に出力する。

また、情報分割回路51は、情報Data1B、Data2B、Data3B、……、DataKB、……、DataNBからなるモジュールD13を暗号化回路53に出力する。

【0044】

暗号化回路52は、所定の暗号鍵を用いて、情報分割回路51から入力した個人情報D12を暗号化して個人情報D14を生成し、これを書き込み回路54に出力する。

暗号化された個人情報D14は、図8に示すように、それぞれ情報Data1A～DataNAを暗号化した情報Data1A'～DataNA'からなる。

【0045】

暗号化回路53は、所定の暗号鍵を用いて、情報分割回路51から入力した個人情報D13を暗号化して個人情報D15を生成し、これを書き込み回路55に出力する。暗号化回路53が用いる暗号鍵は、暗号化回路52が用いる暗号鍵と同じものを用いてもよいし、異なるものを用いてもよい。

暗号化された個人情報D15は、図8に示すように、それぞれ情報Data1B～DataNBを暗号化した情報Data1B'～DataNB'からなる。

【0046】

書き込み回路54は、暗号化回路52から入力したモジュールD14を記録媒体16に書き込む。

【0047】

書き込み回路55は、暗号化回路53から入力したモジュールD15を記録媒体17に書き込む。

【0048】

以下、情報記録装置1の動作を説明する。

図9は、情報記録装置41の動作を説明するためのフローチャートである。

【0049】

ステップST31:

読み出し回路50によって、記録媒体15から図8に示す個人情報D1が読み出されて情報分割回路51に出力される。

【0050】

ステップST32:

情報分割回路51において、図8に示すように、読み出し回路50から入力した個人情報D1が、それぞれを単独では個人情報D1の秘匿性が保持される2つのモジュールD12, D13に分割され、モジュールD12が暗号化回路52に出力され、モジュールD13が暗号化回路53に出力される。

【0051】

ステップST33:

暗号化回路52において、図8に示すように、所定の暗号鍵を用いて、情報分割回路51から入力した個人情報D12が暗号化されて個人情報D14が生成され、これが書き込み回路54に出力される。

また、暗号化回路53において、図8に示すように、所定の暗号鍵を用いて、情報分割回路51から入力した個人情報D13が暗号化されて個人情報D15が生成され、これが書き込み回路55に出力される。



## 【 0 0 5 2 】

ステップ S T 3 4 :

書き込み回路 5 4 によって、暗号化回路 5 2 から入力したモジュール D 1 4 が記録媒体 1 6 に書き込まれる。

書き込み回路 5 5 によって、暗号化回路 5 3 から入力したモジュール D 1 5 が記録媒体 1 7 に書き込まれる。

## 【 0 0 5 3 】

以上説明したように、情報記録装置 4 1 によれば、図 8 に示すように、個人情報 D 1 が、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 1 2, D 1 3 に分割された後に暗号化されてモジュール D 1 4, D 1 5 が生成され、モジュール D 1 4, D 1 5 がそれぞれ物理的に独立した記録媒体 1 6, 1 7 にそれぞれ記録される。

そのため、記録媒体 1 6, 1 7 を別々に保管すれば、記録媒体 1 6, 1 7 の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報 D 1 の秘匿性は保たれる。

## 【 0 0 5 4 】

#### 第 4 実施形態

図 1 0 は、本実施形態の情報復元装置 6 1 の構成図である。

情報復元装置 6 1 は、上述した第 3 実施形態の情報記録装置 4 1 によって、記録媒体 1 6 と 1 7 とに分割して記録された個人情報から、本来の個人情報 D 1 を復元する。

図 1 0 に示すように、情報復元装置 6 1 は、読み出し回路 7 0, 7 1、復号回路 7 2, 7 3、情報合成回路 7 4 および書き込み回路 7 5 を有する。

図 1 0 において、記録媒体 1 6 および 1 7 には、前述した第 3 実施形態で説明した図 9 に示す処理を経て、それぞれモジュール D 1 4 および D 1 5 が記録されている。

## 【 0 0 5 5 】

読み出し回路 7 0 は、記録媒体 1 6 から読み出したモジュール D 1 4 を復号回路 7 2 に出力する。

【0056】

読み出し回路71は、記録媒体17から読み出したモジュールD15を復号回路73に出力する。

【0057】

復号回路72は、読み出し回路70から入力したモジュールD14を、所定の復号鍵を用いて復号してモジュールD12を生成し、これを情報合成回路74に出力する。

【0058】

復号回路73は、読み出し回路71から入力したモジュールD15を、所定の復号鍵を用いて復号してモジュールD13を生成し、これを情報合成回路74に出力する。

【0059】

情報合成回路74は、図11に示すように、復号回路72から入力したモジュールD12と、復号回路73から入力したモジュールD13とを合成して個人情報D1を生成し、これを書き込み回路75に出力する。

【0060】

書き込み回路75は、情報合成回路74から入力した個人情報D1を、記録媒体15に書き込む。

【0061】

以下、情報復元装置61の動作を説明する。

図12は、情報復元装置61の動作を説明するためのフローチャートである。

ステップST41:

読み出し回路70によって、図11に示すように、記録媒体16からモジュールD14が読み出されて復号回路72に出力される。

また、読み出し回路71によって、記録媒体17からモジュールD15が読み出されて復号回路73に出力される。

【0062】

ステップST42:

復号回路72において、読み出し回路70から入力したモジュールD14が、

所定の復号鍵を用いて復号されてモジュールD12が生成され、これが情報合成回路74に出力される。

また、復号回路73において、読み出し回路71から入力したモジュールD15が、所定の復号鍵を用いて復号されてモジュールD13が生成され、これが情報合成回路74に出力される。

【0063】

ステップST43：

情報合成回路74において、図11に示すように、復号回路72から入力したモジュールD12と、復号回路73から入力したモジュールD13とが合成されて個人情報D1が生成され、これが書き込み回路75に出力される。

【0064】

ステップST44：

書き込み回路75によって、情報合成回路74から入力された個人情報D1が、記録媒体15に書き込まれる。

【0065】

以上説明したように、情報復元装置31によれば、正当な者が当該装置を用いることで、前述した第3実施形態の情報記録装置41によって別々の記録媒体16、17に格納されたモジュールD14、D15から個人情報D1を復元できる。

【0066】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、個人情報を分割して得た複数のモジュールを異なる記録媒体に記録する場合を例示したが、当該複数のモジュールを同じ記録媒体の異なる領域に記録してもよい。この場合に、記録媒体の何れの領域に何れもモジュールを記録したかを秘密にしておけば、当該記録媒体を不正に取得した者は、記録媒体から読み出したモジュールの合成の仕方が分からず、個人情報を復元できない。

【0067】

また、上述した実施形態では、所定の情報を分割する前後の何れか一方で暗号

化を行う場合を例示したが、所定の情報を分割する前後の何れでも暗号化を行う場合、並びに所定の情報を分割する前後の双方で暗号化を行う場合でも本発明は適用可能である。

#### 【0068】

また、上述した実施形態では、本発明の所定の情報として、個人情報を例示したが、その他、映像、音声などの情報であってもよい。

#### 【0069】

また、上述した実施形態では、個人情報を2分割して2つの記録媒体16，17に記録する場合を例示したが、個人情報を3分割以上して3つ以上の記録媒体に記録してもよい。

#### 【0070】

#### 【発明の効果】

以上説明したように、本発明によれば、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法およびその装置と、そのような形態で情報が記録された記録媒体とを提供できる。

また、本発明によれば、上述したような情報記録方法およびその装置によって記録媒体に記録された情報を適切に復元できる情報復元方法およびその装置を提供できる。

#### 【図面の簡単な説明】

#### 【図1】

図1は、本発明の第1実施形態の情報記録装置の構成図である。

#### 【図2】

図2は、図1に示す情報記録装置における処理の情報の流れを説明するための図である。

#### 【図3】

図3は、図1に示す情報記録装置の処理のフローチャートである。

#### 【図4】

図4は、本発明の第2実施形態の情報復元装置の構成図である。

#### 【図5】

図5は、図4に示す情報復元装置における処理の情報の流れを説明するための図である。

【図6】

図6は、図4に示す情報復元装置の処理のフローチャートである。

【図7】

図7は、本発明の第3実施形態の情報記録装置の構成図である。

【図8】

図8は、図7に示す情報記録装置における処理の情報の流れを説明するための図である。

【図9】

図9は、図7に示す情報記録装置の処理のフローチャートである。

【図10】

図10は、本発明の第4実施形態の情報復元装置の構成図である。

【図11】

図11は、図10に示す情報復元装置における処理の情報の流れを説明するための図である。

【図12】

図12は、図10に示す情報復元装置の処理のフローチャートである。

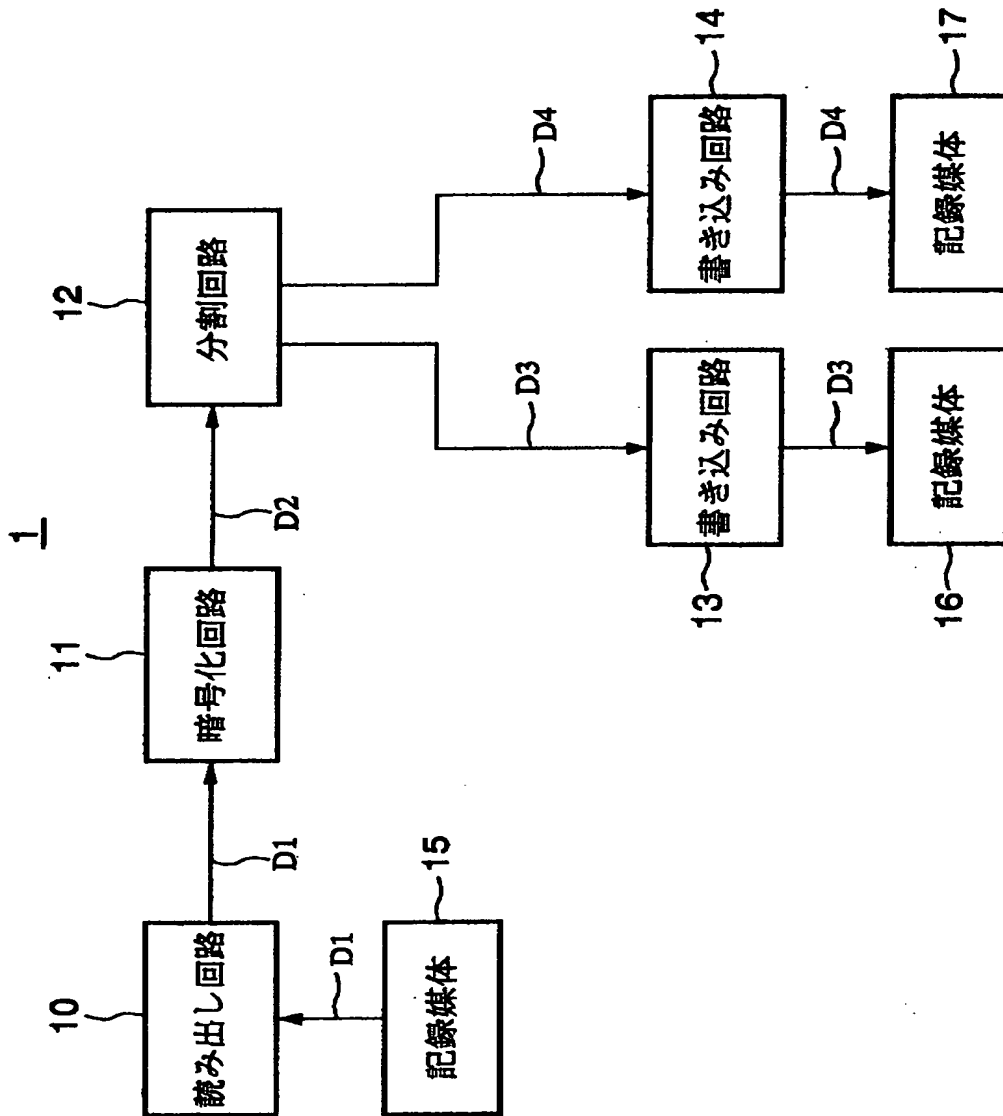
【符号の説明】

1…情報記録装置、10…読み出し回路、11…暗号化回路、12…情報分割回路、13, 14…書き込み回路、15, 16, 17…記録媒体、20, 21…読み出し回路、22…情報合成回路、23…復号回路、24…書き込み回路、31…情報復元装置、41…情報記録装置、50…読み出し回路、51…情報分割回路、52, 53…暗号化回路、54, 55…書き込み回路、61…情報復号装置、70, 71…読み出し回路、72, 73…復号回路、74…情報合成回路、75…書き込み回路

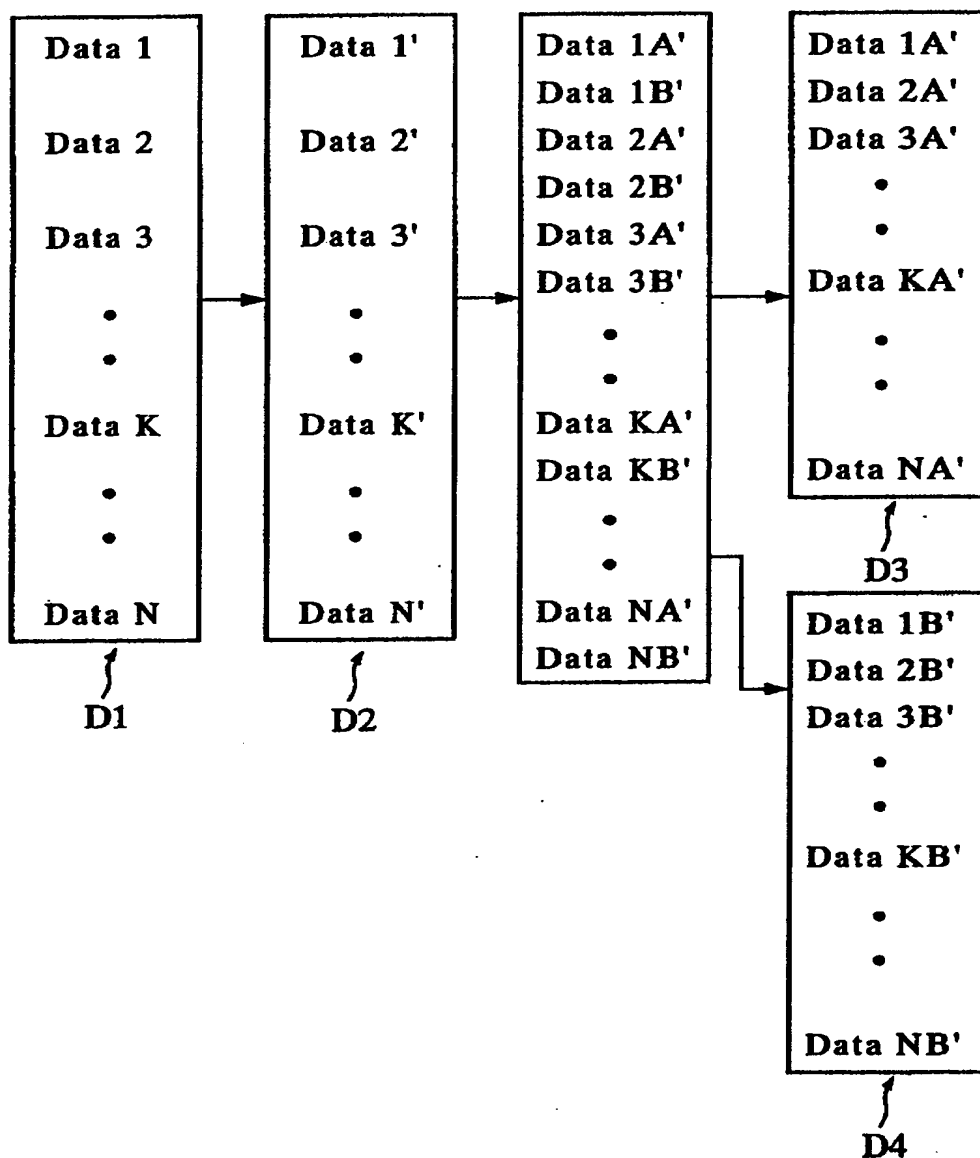
【書類名】

図面

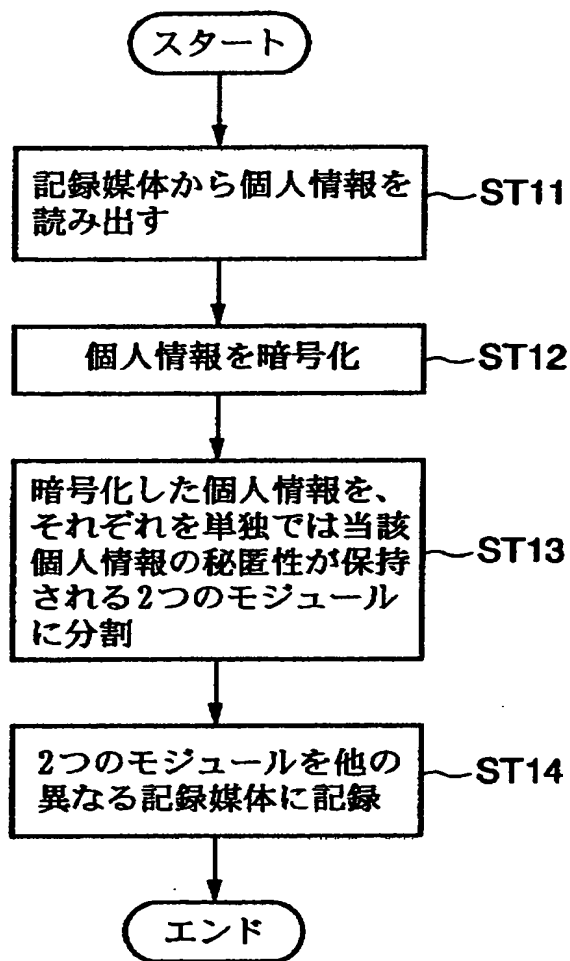
【図 1】



【図 2】

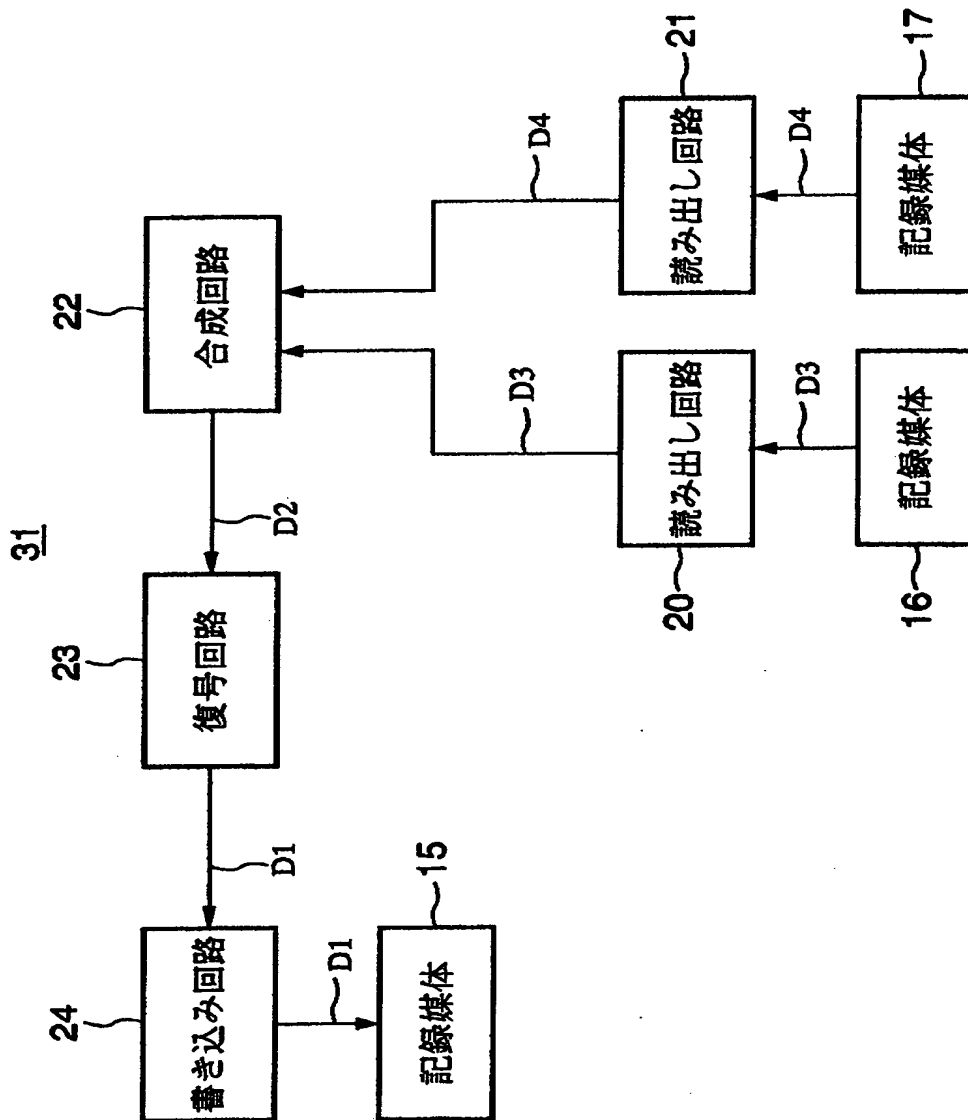


【図3】

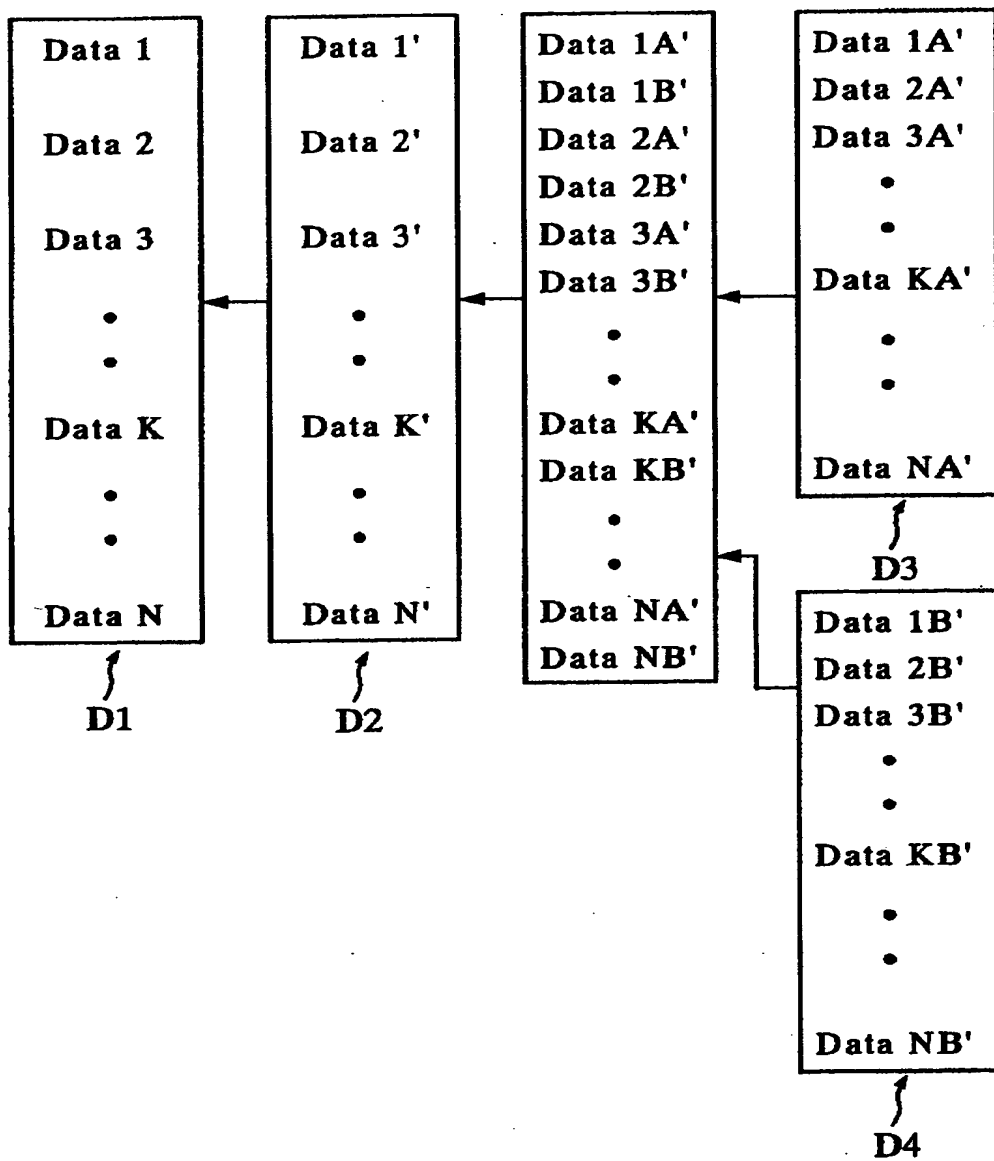




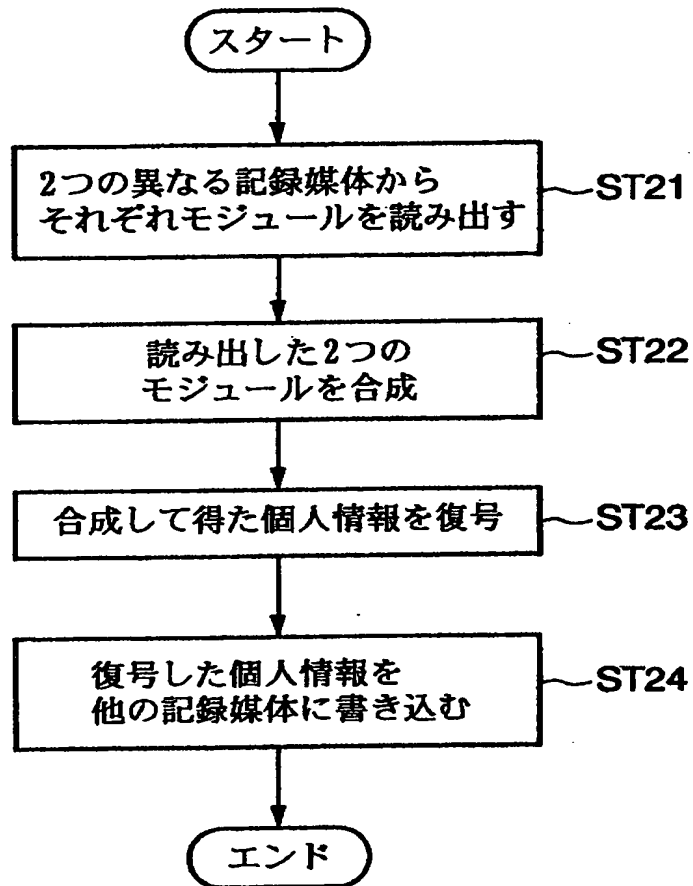
【図 4】



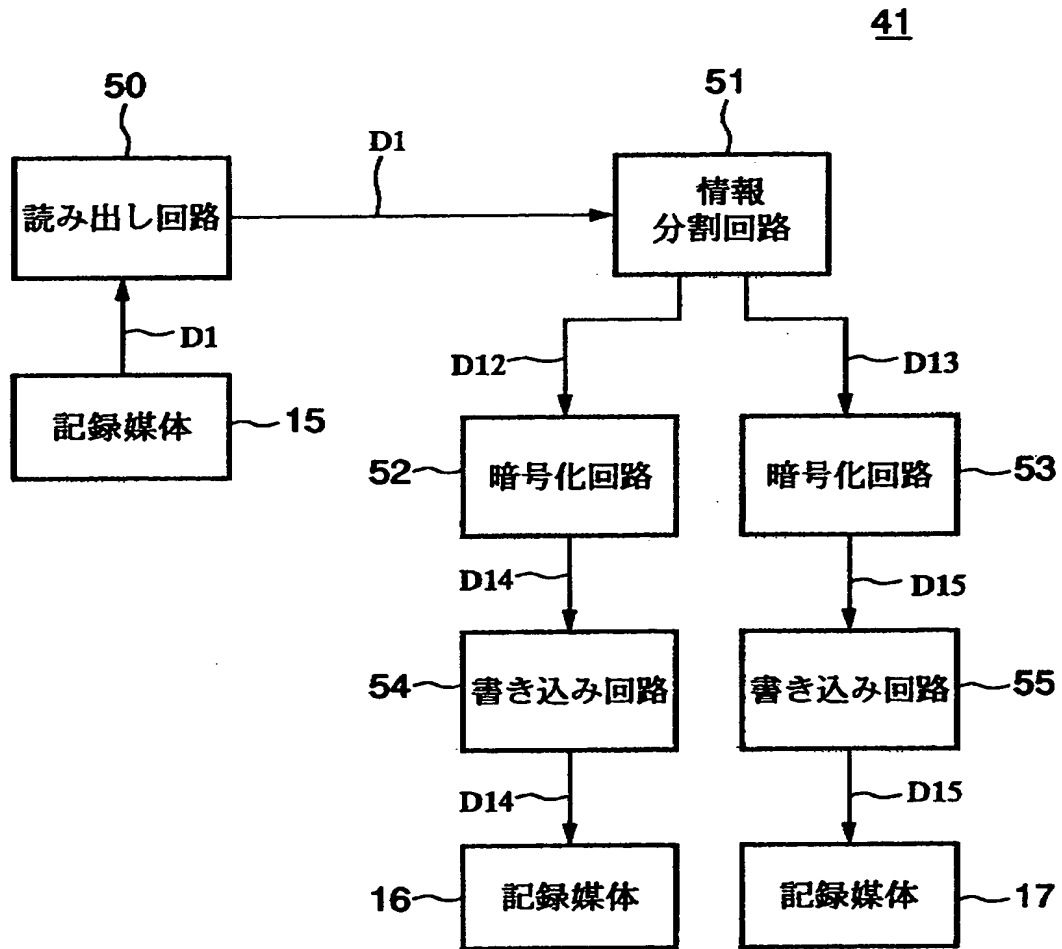
【図 5】



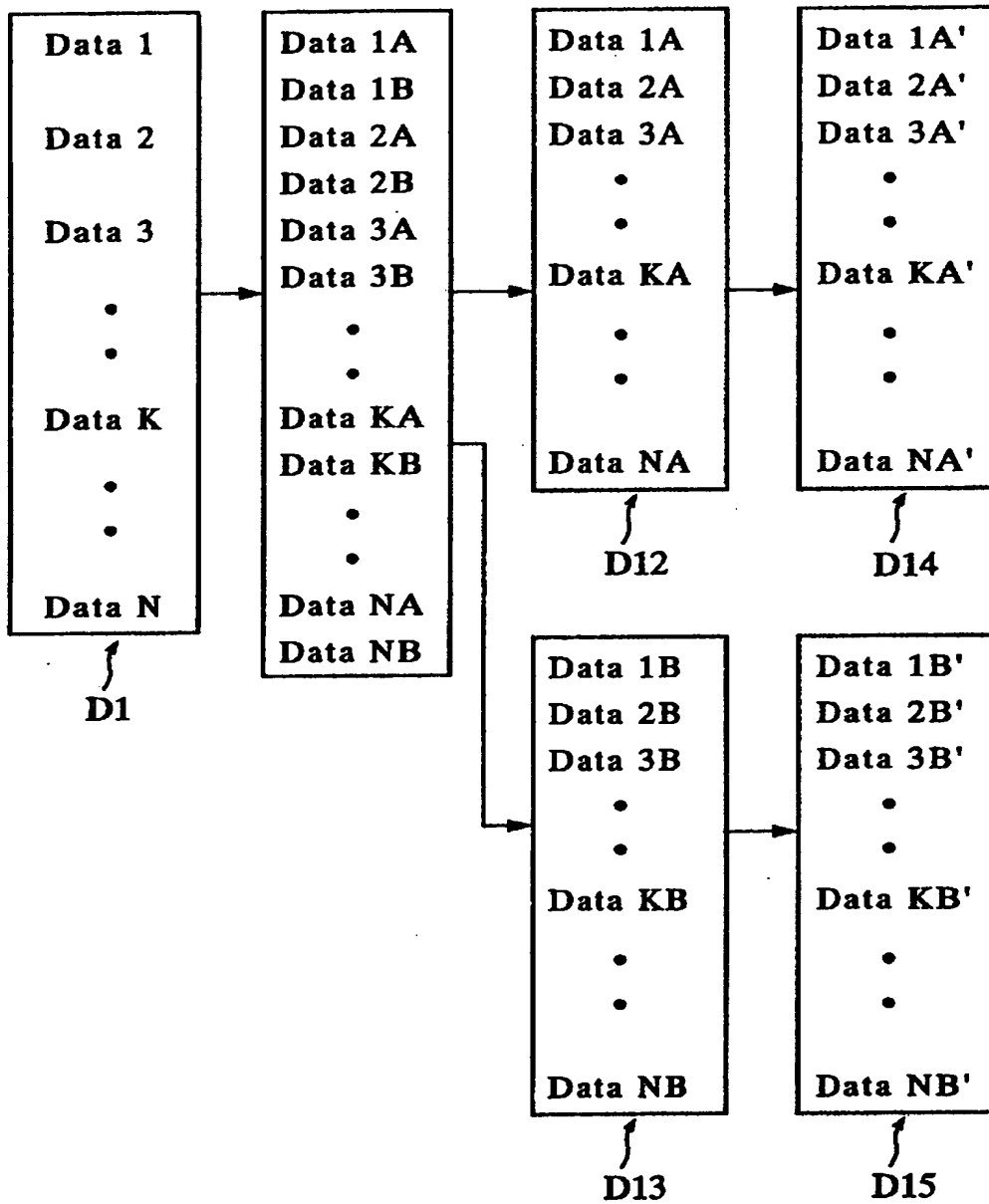
【図6】



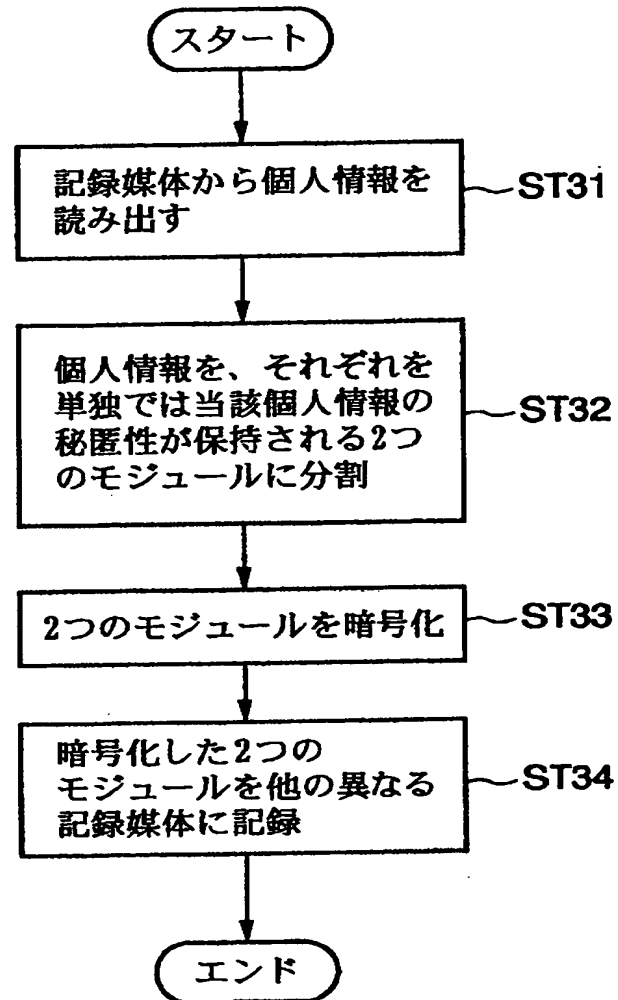
【図 7】



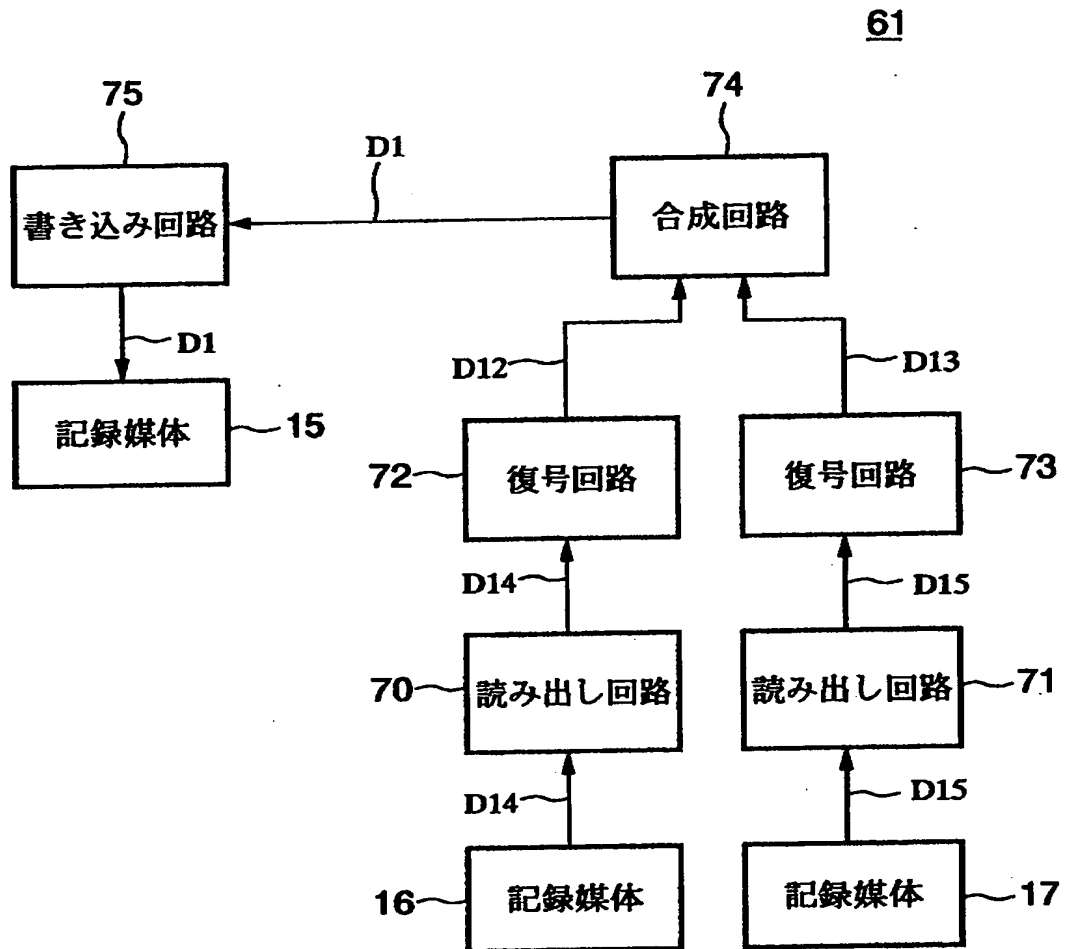
【図 8】



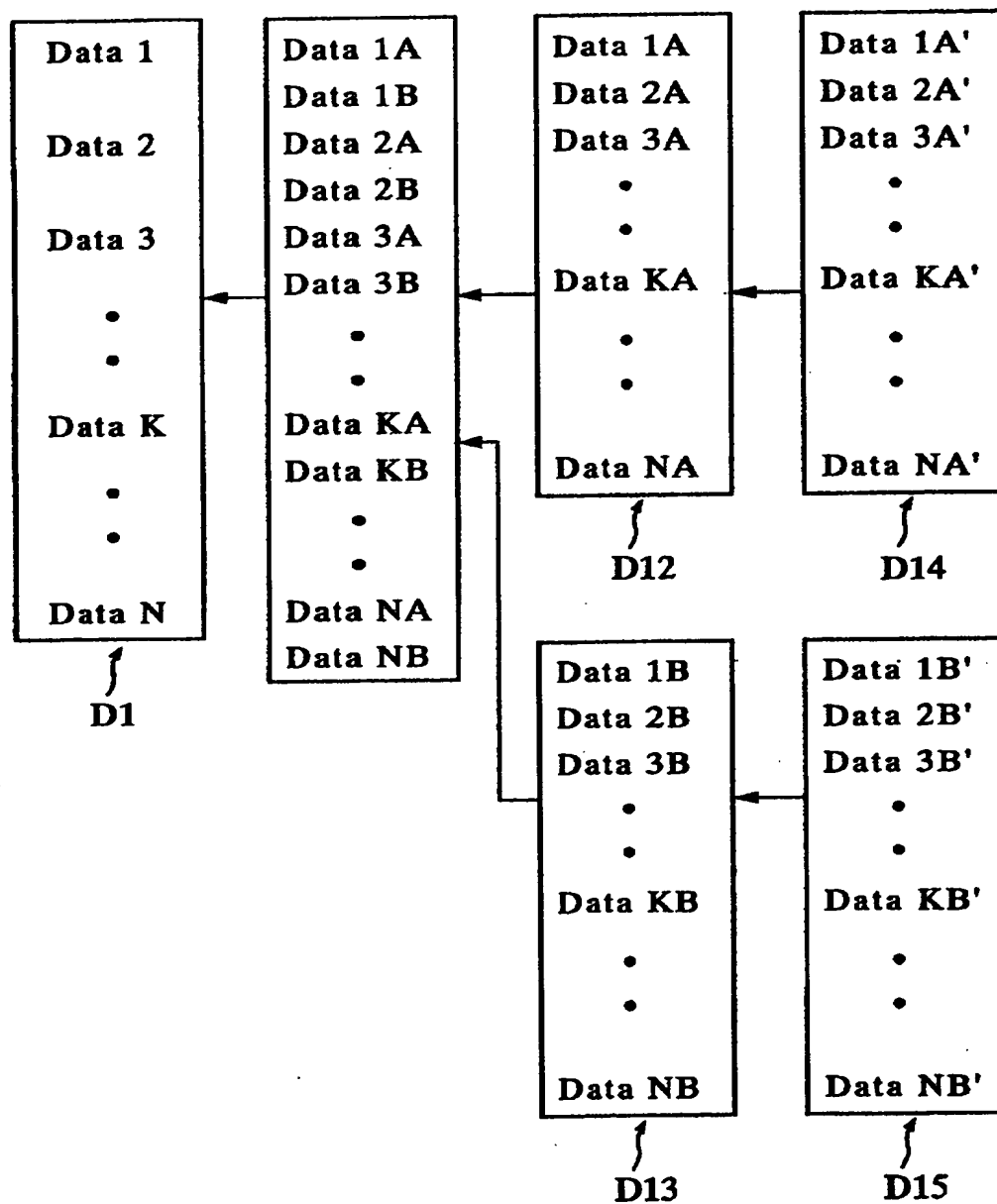
【図9】



【図10】

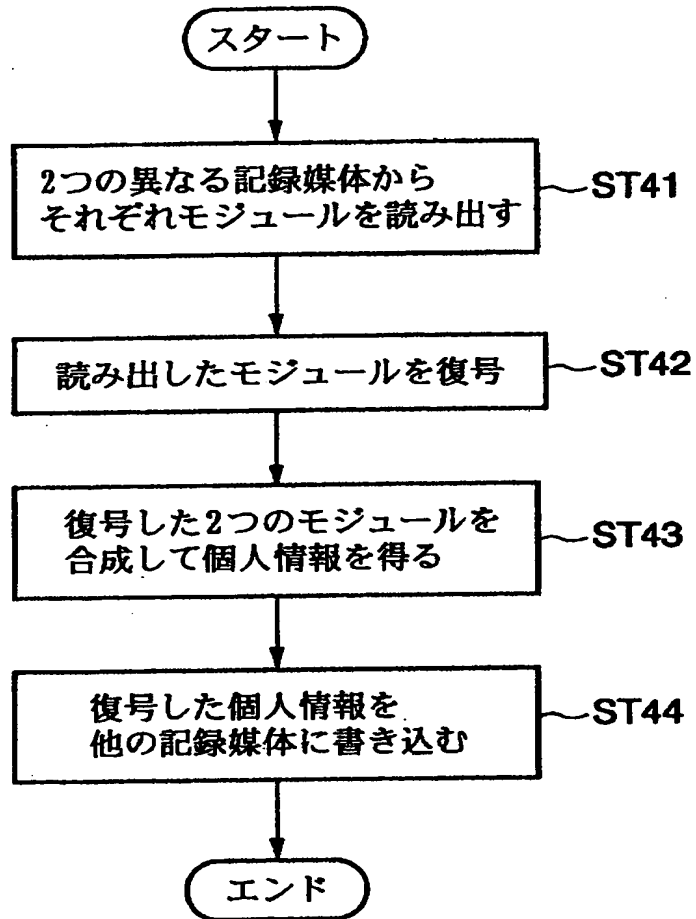


【図 11】





【図12】



【書類名】 要約書

【要約】

【課題】 情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録装置を提供する。

【解決手段】 記録媒体 1 5 から読み出し回路 1 0 によって読み出した個人情報を、情報分割回路 1 2 において、それぞれ単独では当該個人情報の秘匿性が保持される 2 つのモジュール D 3 , D 4 に分割する。書き込み回路 1 3 によって、モジュール D 3 を記録媒体 1 6 に書き込み、書き込み回路 1 4 によってモジュール D 4 を記録媒体 1 7 に書き込む。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

|          |                   |
|----------|-------------------|
| 1. 変更年月日 | 1990年 8月30日       |
| [変更理由]   | 新規登録              |
| 住 所      | 東京都品川区北品川6丁目7番35号 |
| 氏 名      | ソニー株式会社           |

This Page Blank (uspto)